

Appln. No. 09/587,228
Amendment dated January 2, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of September 02, 2003 (Office Action). This response is being filed with a petition for a one month retroactive extension of time with the appropriate fee.

In paragraphs 1-5 of the Office Action, claims 1-2, 11-14, 23-26, 35-38 and 47-48 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Number 6,256,739 to Skopp, *et al.* (Skopp) in view of U.S. Patent Number 6,199,102 to Cobb (Cobb). In paragraphs 6-13 of the Office Action, claims 3-10, 15-22, 27-34, and 39-46 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Skopp in view of Cobb, in further view of U.S. Patent Number 6,537,424 to Dutta (Dutta).

In response to the 35 U.S.C. § 103(a) rejection, Applicants have enclosed affidavits under 37 C.F.R. § 1.131 supporting the removal of Dutta as a reference. The affidavits are accompanied by a copy of the Applicants' confidential invention disclosure entitled "A Method for Preventing Deep Linking into a Web Site". The confidential invention disclosure and affidavits demonstrate proof of conception for the claimed subject matter of the Applicants' invention at least as early as July 28, 1999, which predates the effective date of Dutta. Applicants further exercised due diligence from prior to the effective date of Dutta until June 6, 2000, the filing date of the instant application. Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection with respect to claims 3-10, 15-22, 27-34, and 39-46 is respectfully requested.

Prior to addressing the rejections on the art, a brief review of the Applicants' invention is in order. The Applicants' invention comprises a method for preventing access to a document, such as a Web page, through undesired deep linking. Deep links are hyperlinks specifying a Web page contained in a Web site, which normally can be accessed only by first accessing the home page of the Web site. A user performing "deep linking" can bypass the home page and effectuate the display of the contextually appropriate information by specifying the URL of the interior Web page. In the Applicants' invention, access to a Web page can be provided in an anonymous fashion that is independent of the identity of a user. Instead access is granted or denied based

Appln. No. 09/587,228
Amendment dated January 2, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

upon the source document, where the source document is a Web page containing a hyperlink to the Web page to which user access is desired.

In one embodiment of the Applicants' invention, a request for a Web page can be received by a Web server. The request can contain an identifier used to determine whether to service or deny the request for the Web page. More specifically, the method of the invention can detect within the request the source document of the request by referencing embedded information in a request header contained in the request. The embedded information can be an identifier of the source document, for example a uniform resource locator (URL). Preferably, the URL can be extracted from the request header.

Subsequently, the extracted URL can be compared with an established list or database of source documents represented by their corresponding URLs. The list or database of URLs can represent preferred access points for the requested Web page, whereby the request is serviced only if the referring URL matches one of the URLs in the list or database. Alternatively, the list or database of URLs can represent prohibited access points for the requested Web page, whereby the request is denied if the referring URL matches one of the URLs in the list or database.

Turning to the rejections on the art, in paragraphs 1-5 of the Office Action, claims 1-2, 11-14, 23-26, 35-38 and 47-48 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Skopp in view of Cobb; both of which shall be briefly reviewed before Applicants address the specific issues presented within the Office Action.

Skopp discloses a method and apparatus that includes an access control proxy that a client computer logs onto in order to be granted Internet access, as shown in FIGS. 1A, 1B, 2, 4, and 5 of Skopp. The proxy can determine a user identity and can provide access to a limited set of Web pages based upon the user identity. Skopp is designed as a method through which advertisers can provide free Internet access to users in a limited fashion, where the access limitations are established in a user variable manner. As noted in column 3, lines 34-41 of Skopp, access limitations can depend on demographic information associated with the user, the time of day the Web page request is made, the number of times a user has accessed the Web page, or any

Appln. No. 09/587,228
Amendment dated January 2, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

other factor important to the advertiser. The access control proxy taught by Skopp only limits Internet access to users accessing the Internet via the disclosed proxy; Skopp does not teach or suggest any means for limiting content provided by Web page servers. Nothing taught or suggested by Skopp can resolve the aforementioned problems associated with deep linking. Skopp provides no teachings relating to a content requesting source (calling Web page or source document from which a request originates).

Cobb discloses a method and system for filtering unsolicited e-mail messages. Cobb uses a client-side application disposed within a mail server to filter unsolicited email messages before transferring them to a user's mailbox. More specifically, Cobb, as described in lines 5-8 of the Abstract, teaches receiving a message (that is an email message received by a mail server as noted in FIGS. 2, 3, 4, and 5 of Cobb) from a sender, sending a challenge back to the sender, receiving a response to the challenge, and determining if the response is a proper response. When the response is not proper, the mail server deletes the received e-mail message. When the response is proper, the mail server conveys the received e-mail message to the appropriate user's mailbox.

In Cobb, e-mail filtration is performed by a messaging receiving mail server and is thus performed on the client side of the mail sending-receiving process. Further, the e-mail filters taught by Cobb are linked to user mailboxes and are thus dependant upon user identity. Nothing taught or suggested by Cobb can resolve the aforementioned problems associated with deep linking. Cobb does not address a situation where a request for content is made to a content server in any manner. Cobb provides no teachings relating to a content requesting source (calling Web page or source document from which a request for a different Web page originates).

In paragraph 3 of the Office Action, regarding claim 1 and the associated apparatus claim 25, the Examiner contends that Skopp teaches establishing a list of sources from which a request to access a document (Web page) can originate, receiving a request from a requesting client, detecting in the request the identity of a source of the request, and servicing the request if the detected identity matches an

Appln. No. 09/587,228
Amendment dated January 2, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

allowable source document contained in the list. In support, the Examiner has cited column 6, line 65 through column 7, line 27 and column 8, line 19 through column 9 line 27 of Skopp. While the cited passage does teach that Web pages can be added to an Access Control List (ACL), the ACL list is not equivalent to or suggestive of the list of allowable source documents from which a request for Web access can originate.

Specifically, in Skopp, the ACL is maintained by the access control proxy 310 (column 7, lines 2 and 3). The access control proxy 310 according to column 7, lines 14-16 can limit a user's Web access based on the identity of the user or the specific advertisement being requested (by that user). Each ACL list is a user specific list. Further, the ACP and the associated ACL list is a client side list, as indicated by FIGS. 1A, 1B, and 2 of Skopp, that contains a listing of Web sites that a particular client cannot access; other Internet users can access the Web sites contained within the ACL list. In contrast, the list of documents of claim 1 of the Applicants' invention is a server-side list, as indicated by FIG. 4 of the Applicants' invention, that prevents a Web server from providing content to any user. The access control proxy that prevents users from accessing the Internet and/or specific Internet Web pages is very different from a method for "preventing access to a document in a server", i.e. selectively serving Web pages, as claimed by the Applicants.

Further, in the Applicants' invention, the specified list contains allowable source documents from which a request to access a document can originate. The source document can contain a hyperlink to the requested document. The request can include embedded information identifying the source document, such as a URL. Accordingly, a Web server can prevent deep linking based upon the source document from which a request is made. The Examiner has acknowledged in paragraph 3 that Skopp does not teach a method that prevents access based on an identity of a source document.

The Examiner contends, however, that Cobb teaches using a source document for controlling Internet access. In support, the Examiner cites column 2, lines 26-46 and column 3 lines 10-50 of Cobb. The cited passages of Cobb, however, refer to electronic messages, such as email, that have already been sent by transmitting mail server to a recipient mail server. The source discussed by Cobb refers to the identity of the

Appln. No. 09/587,228
Amendment dated January 2, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

transmitting mail server or transmitting e-mail account. Cobb never teaches that a source document can be a Web page containing a hyperlink to a target Web page. Moreover, Cobb includes no teachings pertinent to accessing Web pages in any fashion. Unlike the Applicants' invention, Cobb provides no teachings applicable to the problem of deep linking.

In paragraph 4 of the Office Action, claims 13 and 37 have been rejected for substantially the same reasons as claims 1 and 25 have been rejected in paragraph 3. Claims 13 and 37 establish an exclusionary list of source documents from which a request to access a document cannot originate. That is, claims 13 and 37 provide access control to Web pages by denying access using a list of prohibited source documents as opposed to granting access based on a list of permitted source documents. As stated above in the Applicants' response to claims 1 and 25, neither Skopp, Cobb, nor any combination of the two teach or suggest preventing access to Web pages in an anonymous fashion based upon the identity of a source document. Instead, both rely upon an identity of a user. Accordingly, claims 13 and 37 should be allowable claims over Skopp-Cobb for the same reasons that claims 1 and 25 should be allowable.

In paragraph 5 of the Office Action, claims 2, 11, 12, 14, 24, 25, 26, 35, 36, 38, 47 and 48 have been rejected based upon Skopp-Cobb. The Examiner has not cited any passages from Skopp or Cobb that teach or suggest preventing a Web server from serving documents as specified by claims 2, 14, 26, and 38. Both Skopp and Cobb are client side applications, which have nothing to do with a server-side limitation. Further, claims 11, 12, 24, 25, 35, 36, 47, and 48 relate to either not serving a requested document based upon an identity of a source document or serving a substitute document based upon an identity of a source document. Again, both Skopp and Cobb are client side applications, which have nothing to do with server-side restrictions.

Applicants note that no rationale has been provided in paragraph 5 of the Office Action for rejecting claims 2, 11, 12, 14, 24, 25, 26, 35, 36, 38, 47 and 48. Applicants further note that paragraph 5 of the Office action appears incomplete. Applicants

Appln. No. 09/587,228
Amendment dated January 2, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

cannot, therefore, provide a meaningful response to the rejections of paragraph 5 beyond the general response presented above.

Even if a combination of Skopp and Cobb taught or suggested claimed limitations of the Applicants' invention, which is not true for the reasons stated above, there is no motivation to combine the teachings of Skopp and Cobb. Skopp teaches a method for limiting Internet access using an access control proxy. Cobb teaches a method for filtering received e-mail messages after the e-mail messages have been received by a mail server. Further, neither Skopp nor Cobb includes methodologies for preventing a Web server from serving Web pages as disclosed in the Applicants' invention. Absent the Applicants' own disclosure, prior art fails to provide any teachings or suggestions relevant to serving Web content.

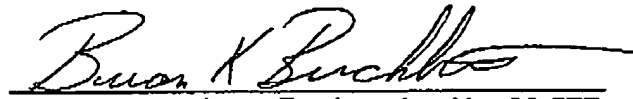
Further, Applicants respectfully submit that the prior art of record fails to express the desirability to combine the teachings of Skopp with the teachings of Cobb in the manner suggested by the Examiner. As noted in *In re Gordon*, 733 F.2d 099, 221 USPQ at 1127 "the mere fact that prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggests the desirability of the modification." Absent such a suggestion, it is improper to combine the references of Skopp and Cobb, particularly in light of the fact that each is a client side methodology and is dependant upon user identity; two limitations, which teach away from the Applicants' invention of an anonymous, server side content control methodology.

Appln. No. 09/587,228
Amendment dated January 2, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: 31 Dec 2003

Gregory A. Nelson, Registration No. 30,577
Kevin T. Cuenot, Registration No. 46,283
Brian K. Buchheit, Registration No. 52,667
AKERMAN SENTERFITT
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000